Foresthill Telephone Co.

DOCKET FILE COPY ORIGINAL

Received & Inspected

FEB 19 2008

FCC Mail Room

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 15, 2008

Name of company covered by this certification: Foresthill Telephone Co.

Form 499 Filer ID: 807798

Name of signatory: Al Baumgarner

Title of signatory: Chief Financial Officer

I, Al Baumgarner, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions against data brokers in the past year as it has not had any instances of CPNI infractions.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI .

Signed

Al Baumgarner

No. of Copies rec'd 1
List ABCDE

P.O. Box 1189
Foresthill, California 95631
Tel. 530.367.2222
www.foresthilltelephone.com

CPNI OPERATING GUIDELINES

Foresthill Telephone Co. (Company) adheres to the following guidelines:

General Company Policies

The Company uses, discloses, or permits access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

The Company uses, discloses, or permits access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.*, local, interexchange, DSL, etc.) to which the customer already subscribes from the Company, without customer approval.

The Company shares CPNI only among the carrier's affiliated entities that provide a service offering to the customer. Except as noted herein, the Company shares CPNI with its affiliates only when it has approval from the customer through an opt-in or opt-out process as appropriate per FCC rules.

The Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, the Company does not use local service CPNI to track all customers that call local service competitors.

Company Policy Governing the Approval Required for Use of Customer Proprietary Network Information.

The Company obtains approval through written, oral or electronic methods, and we understand that the Company bears the burden of demonstrating that such approval has been given in compliance with the applicable FCC Rules.

The customer's approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by the Company remains in effect until the customer revokes or limits such approval or disapproval.

The Company may seek alternatively either "opt-in" or "opt-out" approval consistent with applicable FCC requirements in order to obtain authorization to use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. The Company, subject to appropriate customer approval, may disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents; its affiliates that provide communications-related services; and its joint venture partners and independent contractors. The Company also permits such persons or entities to obtain access to such CPNI for such purposes. Disclosure to or access provided to joint venture partners and

independent contractors is undertaken in compliance with Joint Venture/Contractor safeguards set forth below:

Joint Venture/Contractor Safeguards: The Company discloses or provides access to CPNI to its joint venture partners or independent contractors that comply with the following requirements:

(i) Require that the independent contractor or joint venture partner use the CPNI only for the purpose of marketing or providing the communications-related services for which that CPNI has been provided;

(ii) Disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; and

(iii) Require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumers' CPNI.

Company Policies Regarding the Notice Required for Use of Customer Proprietary Network Information.

Prior to any solicitation for customer approval, the Company provides clear and comprehensive notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. These notifications are retained for at least one year. Customers are provided notice and sufficient information for them to make an informed decision when soliciting approval to use, disclose, or permit access to customers' CPNI. The notification states that the customer has a right, and the Company has a duty, under Federal law, to protect the confidentiality of CPNI and identifies the types of information that constitute CPNI and purposes for which it will be used.

Such notice informs the customer of his or her right to disapprove those uses, as well as the steps the customer must take in order to grant or deny access to CPNI. Notices state clearly that a denial of approval will not affect the provision of any services to which the customer subscribes but may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI, *i.e.*, lack of ability to market certain services that may be of interest to the subscriber.

The Company waits at least 30 days after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI.

The Company uses oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call,

regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

Company Policies Regarding Safeguards for Use of Customer Proprietary Network Information.

The Company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

The Company trains its personnel as to when they are and are not authorized to use CPNI, and the Company has an express disciplinary process in place.

The Company maintains a record of sales and marketing campaigns that use customers' CPNI. The Company maintains a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. The Company retains the record for a minimum of one year.

The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly. The notice will be in the form of a letter, and will include the Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information. This notice will be submitted even if the carrier offers other methods by which consumers may opt-out.

Company Policies Regarding Safeguarding Privacy of Customer Proprietary Network Information.

Release of customer CPNI information is only be provided when: customers initiating telephone call provide the password of record; request the information to be sent via mail USPS to the customer's address of record; or by calling the telephone number of record and disclose the CPNI information.

Customers CPNI information is also provided at the FTC business office when Customer of record can provide valid, government issued photo identification, such as a driver's license, passport, or comparable ID issued identification or with their password. The Company currently does not allow on line access to customer CPNI information.

The Company will notify customer immediately of any account changes including password, customer response to company designed back-up means of

authentication, on-line account, address of record, and any other record that may be created or changed. This notification will be through a voicemail or by USPS mail to the address of record as it was prior to the change.

All customer complaints concerning the unauthorized release of CPNI will be logged and retained for a period of five years. This information is summarized in the reporting information below.

Any CPNI breaches are reported within seven (7) days after a reasonable determination of a breach has occurred to law enforcement officials. Should a breach occur, an electronic notification will be sent through the central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). Notification will include a description of the CPNI that was disclosed, how the breach was discovered, an analysis of the sensitivity of the breached CPNI, and any corrective measures taken to prevent recurrence of such breach.

Customer notification of a breach is provided to the customer after 7 days unless alternative direction is provided by law enforcement officials or unless extraordinarily urgent notification is required to avoid immediate and irreparable harm.

The company also utilizes multiple layers of security to protect its customer CPNI databases and systems from outside sources including industry-standard firewalls endpoint security, limitation of access to Company systems, password-protected and encryption. The Company reviews its cyber systems periodically to determine if more advanced protection methods are available.

The Company trains its personnel as to privacy issues, pretexting, and when and under what circumstances they can disclose CPNI information to customers. The Company has an express disciplinary process in place for intentional or unintentional breaches of information.

Relevant Reporting Information

The Company had no reported customer complaints concerning the release of unauthorized CPNI information.

The Company had no unauthorized breaches of CPNI information.

The Company had no reportable instances where its opt-out policy did not work appropriately.

The Company has not taken any action against data brokers as no breaches have occurred during this period.